SCRAMBLE COMMUNICATION METHOD AND SYSTEM THEREFOR

Patent Number: JP9321750
Publication date: 1997-12-12
Inventor(s): SHIROSHITA TERUJI
Applicant(s):: NIPPON TELEGR & TELEPH CORP <NTT>
Requested Patent: ☐ JP9321750
Application Number: JP19960328617 19961209
Priority Number(s):
IPC Classification: H04L9/34 ; H04H1/02 ; H04K1/06 ; H04N7/167
EC Classification:
Equivalents:

Abstract

PROBLEM TO BE SOLVED: To reduce processing amount and processing time which are necessary for scrambling processing and restore processing by dividing data into plural data units being a packet size, giving a false packet identifier which indicates scrambled packet order, assembling a packet and executing transmission to a network by means of the packet order which is scrambled based on the false packet identifier.
SOLUTION: Whole data is scrambled and divided into a proper packet size in packet transmission with scrambling (P1(S1)). A false packet identifying number pfx is directly calculated from the memory address of division data in the respective packets so as to be given to the respective packets and, while executing this, the packet is assembled. (P2(S2) and S3). In the meantime, in packet reception while executing restoration, the packet is received while directly calculating the memory address of division data from the false packet identifying number pfx(D1). Then, whole original data is re-constituted based on the memory address of division data (R1(D2)).

【特許請求の範囲】

【請求項１】　ネットワークで接続された送信側と受信側間のスクランブル通信方法であって、
送信側において、元のデータをパケットサイズの複数のデータ単位に分割し、該データ単位をパケットに格納して該パケットにスクランブルしたパケット順序を示す偽のパケット識別子を付与して該パケットを組み立て、該パケットを該偽のパケット識別子に基づいてスクランブルしたパケット順序でネットワークに送信することにより、該元のデータをスクランブルするステップと、
受信側において、前記偽のパケット識別子から真のデータ単位順序を示すデータ単位順序情報を復元し、前記パケットに格納された前記データ単位から該データ単位順序情報に基づいて前記元のデータを再構成することにより、ネットワークから受信した前記パケットを復元するステップと、
を有することを特徴とするスクランブル通信方法。

【請求項２】　前記スクランブルするステップは、スクランブルされていないパケット順序を示す真のパケット識別子を前記パケットに付与し、所定のスクランブルキーに基づいて該真のパケット識別子を前記偽のパケット識別子に置き換えることにより該パケットを組み立て、
前記復元するステップは、前記所定のスクランブルキーに対応する所定のアセンブルキーに基づいて前記偽のパケット識別子を前記真のパケット識別子に変換し、前記元のデータを再構成するにあたって該真のパケット識別子を前記データ単位順序情報として用いることにより該データ単位順序情報を復元する、
ことを特徴とする請求項１記載のスクランブル通信方法。

【請求項３】　前記スクランブルするステップは、所定の計算手順に基づいて前記データ単位のメモリアドレスから前記偽のパケット識別子を直接計算して前記パケットを組み立て、
前記復元するステップは、所定の計算手順に基づいて前記の偽パケット識別子から前記データ単位のメモリアドレスを直接計算し、前記元のデータを再構成するにあたって該メモリアドレスを前記データ単位順序情報として用いることにより該データ単位順序情報を復元する、
ことを特徴とする請求項１記載のスクランブル通信方法。

【請求項４】　前記スクランブルするステップは、送信側におけるプロトコル処理により行われることを特徴とする請求項１記載のスクランブル通信方法。

【請求項５】　前記復元するステップは、受信側におけるプロトコル処理により行われることを特徴とする請求項１記載のスクランブル通信方法。

【請求項６】　前記スクランブルするステップは、前記パケットを送信する処理中に利用可能な空き時間を利用して前記元のデータの分割と前記パケットの組み立てを行うことを特徴とする請求項１記載のスクランブル通信方法。

【請求項７】　前記復元するステップは、前記パケットを受信する処理中に利用可能な空き時間を利用して前記データ単位順序情報の復元と前記元のデータの再構成を行うことを特徴とする請求項１記載のスクランブル通信方法。

【請求項８】　前記スクランブルするステップは、所定の数の前記パケットをまとめて送信し、前記元のデータが該所定の数で割切れないときには、該スクランブルするステップは、少なくとも一つのパディングパケットを挿入してまとめて送信する該所定の数のパケットを形成することにより該パケットを組み立てることを特徴とする請求項１記載のスクランブル通信方法。

【請求項９】　受信側から送信側に、未受信のパケットの偽のパケット識別子を示す否定応答を送るステップと、
送信側から受信側に、該否定応答に示された偽のパケット識別子に基づいて、該未受信パケットに該当する偽の識別子を有するパケットを再送するステップと、　を更に有することを特徴とする請求項１記載のスクランブル通信方法。

【請求項１０】　ネットワークに設けられた中継装置において、該中継装置に設けられ、各パケット中に指定された宛先に対応する次の転送先または最終宛先を示す宛先変換テーブルに基づいて、各パケット中に指定された宛先を変更して、送信側から送信された前記パケットを中継するステップ、
を更に有することを特徴とする請求項１記載のスクランブル通信方法。

【請求項１１】　ネットワークと、
元のデータをパケットサイズの複数のデータ単位に分割し、該データ単位をパケットに格納して該パケットにスクランブルしたパケット順序を示す偽のパケット識別子を付与して該パケットを組み立てることにより該元のデータをスクランブルするスクランブル処理手段と、該パケットを該偽のパケット識別子に基づいてスクランブルしたパケット順序でネットワークに送信する送信手段と、
を含む前記ネットワークに接続された送信装置と、
前記ネットワークから前記パケットを受信する受信手段と、前記偽のパケット識別子から真のデータ単位順序を示すデータ単位順序情報を復元し、該パケットに格納された前記データ単位から該データ単位順序情報に基づいて前記元のデータを再構成することにより、該パケットを復元する復元処理手段と、を含む前記ネットワークに接続された受信装置と、
を有することを特徴とするスクランブル通信システム。

【請求項１２】　前記スクランブル処理手段は、スクランブルされていないパケット順序を示す真のパケット識別子を前記パケットに付与し、所定のスクランブルキー

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開平9－321750
(43)公開日　平成９年(1997)12月12日

(51)Int.Cl.⁶	識別記号	庁内整理番号	Ｆ Ｉ		技術表示箇所
Ｈ０４Ｌ　9/34			Ｈ０４Ｌ　9/00	６８１	
Ｈ０４Ｈ　1/02			Ｈ０４Ｈ　1/02	Ｅ	
Ｈ０４Ｋ　1/06			Ｈ０４Ｋ　1/06		
Ｈ０４Ｎ　7/167			Ｈ０４Ｎ　7/167	Ｚ	

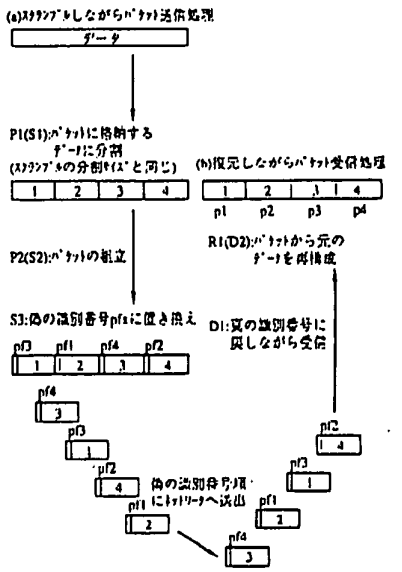
審査請求　未請求　請求項の数20　ＯＬ　（全 18 頁）

(21)出願番号　特願平8－328617
(22)出願日　平成８年(1996)12月９日
(31)優先権主張番号　特願平7－320903
(32)優先日　平７(1995)12月８日
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平8－77602
(32)優先日　平８(1996)３月29日
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号
(72)発明者　城下　輝治
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　弁理士　三好　秀和　（外１名）

(54)【発明の名称】　スクランブル通信方法及びシステム

(57)【要約】
【課題】　送信側や受信側におけるスクランブル処理や復元処理に必要な処理量や処理時間を軽減することが可能なスクランブル通信方法およびシステムを提供すること。
【解決手段】　送信側においては、元のデータをパケットサイズの複数のデータ単位に分割し、データ単位をパケットに格納して該パケットにスクランブルしたパケット順序を示す偽のパケット識別子を付与して該パケットを組み立て、パケットを偽のパケット識別子に基づいてスクランブルしたパケット順序でネットワークに送信することより、元のデータをスクランブルする。受信側においては、偽のパケット識別子から真のデータ単位順序を示すデータ単位順序情報を復元し、パケットに格納されたデータ単位から該データ単位順序情報に基づいて元のデータを再構成することにより、ネットワークから受信した前記パケットを復元する。



ット）を受け取り、データ受信部１２２０において、受信した転送データ単位（パケット）からデータA'を再構成する。

【０００５】そして、アプリケーション部１２１０においてデータA'に復元処理を行い元のデータA全体を復元する。

【０００６】尚、データ通信では、通常、サーバにおいて、送信データを分割して各転送データ単位（パケット）に識別番号を付与して転送し、データの送受信管理を行う。

【０００７】

【発明が解決しようとする課題】しかしながら、上記の従来の方法では、送信装置において、例えば、データ転送前のファイル全体にスクランブルをかけるために、長時間を要する。また、同様に、受信装置において、受信したデータ全体を元の状態に復元するのにも長時間を要するため、利用者が受信したデータを取得するために時間がかかると共に煩わしいという問題がある。

【０００８】ここで、図２および図３を参照して、従来のスクランブル配送を用いたデータ転送方式を更に詳しく説明する。

【０００９】図２に示すように、従来のシステムでは、送信側はスクランブル処理（Ｓ１，Ｓ２，Ｓ３）を行うアプリケーション２１００と送信処理（Ｐ１，Ｐ２）を行うプロトコル処理部２２００を有し、受信側は受信処理（Ｒ１）を行うプロトコル処理部２４００と復元処理（Ｄ１，Ｄ２）を行うアプリケーション２５００とを有し、送信側と受信側は通信ネットワーク２３００を介して接続される。

【００１０】各部で行われる処理は、図３に示すように、以下の通りである。

【００１１】（１）スクランブル処理

Ｓ１：データ全体を適当な分割サイズに分割する。

【００１２】Ｓ２：シーケンス番号やメモリアドレス等のデータ識別番号（図３中で各分割データにつけられた数字）をＳ１で得た各分割データに付与する、または各分割データに割当てて別途管理する。

【００１３】Ｓ３：分割データとそのデータ識別番号を所定のスクランブルキーに基づいて置き換える。

【００１４】（２）送信処理

Ｐ１：送信するデータをパケットに格納する。ここで、パケットサイズは上記スクランブル処理（１）で用いた分割サイズとは異なる。

【００１５】Ｐ２：順序を持ったパケット識別番号（シーケンス番号）ｐｘを順序照合や再送等の送受信管理のためにパケットに付ける。

【００１６】その後パケットは送信側から通信ネットワーク２３００に送信され、受信側で受信される。一般に、受信パケットはネットワーク中で順序が入れ替わり、送信した通りの順序で受信側には届かない。

【００１７】（３）受信処理

Ｒ１：受信パケットを所定のアセンブルキーに基づいて正しいアドレスに格納して、データ全体を再構成する。

【００１８】（４）復元処理

Ｄ１：パケットに格納された分割データの元のデータ識別番号を所定のアセンブルキーに基づいて復元する。

【００１９】Ｄ２：復元された元のデータ識別番号に基づいて分割データの順序を入れ替えて元のデータを復元する。

【００２０】尚、送信処理Ｐ１，Ｐ２と受信処理Ｒ１のプロトコル処理はスクランブル配送をするかしないかに拘らずパケットによるデータ通信では必須の処理である。

【００２１】この図３に示す従来の方式では、送信処理とは別にスクランブル処理を行い、受信処理とは別に復元処理を行っている。このため、従来のスクランブル配送を用いたデータ転送方式では、スクランブル処理、復元処理の全体が追加の処理量と処理時間を必要とするものであった。

【００２２】また、従来はネットワーク加入者の設備（サーバ、端末）と接続している回線設備と中継を行うネットワーク設備が単一の通信事業者内で閉じられたネットワークで運用されているが、近年、ネットワークのインタフェースが多数の通信事業者やＶＡＮ業者（付加価値通信業者）にも開示され、複数事業者により設備間が結合された複合的なネットワークが提供されつつある。従来の単一業者内のネットワークでは、加入者回線、中継設備等の物理的なネットワーク自体が外部からのアクセスが難しく、また、設備間のインタフェースも公開されていなかったので、通信データの機密性が守られている。しかし、複数業者によるサービスの場合は、各業者設備間の接続点、あるは、各業者の中継設備と端末接続している回線との接続点において、非登録利用者から無断で通信データが取得される可能性がでてきている。

【００２３】本発明は、上記課題に鑑みてなされたもので、送信側や受信側におけるスクランブル処理や復元処理に必要な処理量や処理時間を軽減することが可能なスクランブル通信方法およびシステムを提供することを目的とする。

【００２４】また、本発明は、複数のネットワークが接続された複合的なネットワークを用いる場合に信頼性の高い情報通信サービスを実現することが可能なスクランブル通信方法およびシステムを提供することを目的とする。

【００２５】

【課題を解決するための手段】本発明は、ネットワークで接続された送信側と受信側間のスクランブル通信方法であって、送信側において、元のデータをパケットサイズの複数のデータ単位に分割し、該データ単位をパケットに基づいて該真のパケット識別子を前記偽のパケット識別子に置き換えることにより該パケットを組み立て、

前記復元処理手段は、前記所定のスクランブルキーに対応する所定のアセンブルキーに基づいて前記偽のパケット識別子を前記真のパケット識別子に変換し、前記元のデータを再構成するにあたって該真のパケット識別子を前記データ単位順序情報として用いることにより該データ単位順序を復元する、ことを特徴とする請求項１１記載のスクランブル通信システム。

【請求項１３】　前記スクランブル処理手段は、所定の計算手順に基づいて前記データ単位のメモリアドレスから前記偽のパケット識別子を直接計算して前記パケットを組み立て、

前記復元処理手段は、前記所定の計算手順に基づいて前記偽のパケット識別子から前記データ単位のメモリアドレスを直接計算し、前記元のデータを再構成するにあたって該メモリアドレスを前記データ単位順序情報として用いることにより該データ単位順序情報を復元する、ことを特徴とする請求項１１記載のスクランブル通信システム。

【請求項１４】　前記スクランブル処理手段は、前記元のデータの分割と前記パケットの組み立てをプロトコル処理を実行することにより行うことを特徴とする請求項１１記載のスクランブル通信システム。

【請求項１５】　前記復元処理手段は、前記データ単位順序情報の復元と前記元のデータの再構成をプロトコル処理を実行することにより行うことを特徴とする請求項１１記載のスクランブル通信システム。

【請求項１６】　前記スクランブル処理手段は、前記送信手段による前記パケットを送信する処理中に利用可能な空き時間を利用して前記元のデータの分割と前記パケットの組み立てを行うことを特徴とする請求項１１記載のスクランブル通信システム。

【請求項１７】　前記復元処理手段は、前記受信手段による前記パケットを受信する処理中に利用可能な空き時間を利用して前記データ単位順序情報の復元と前記元のデータの再構成を行うことを特徴とする請求項１１記載のスクランブル通信システム。

【請求項１８】　前記送信手段は、所定の数の前記パケットをまとめて送信し、前記元のデータが所定の数で割切れないときには、前記スクランブル処理手段は、少なくとも一つのパディングパケットを挿入してまとめて送信する該所定の数のパケットを形成することにより該パケットを組み立てることを特徴とする請求項１１記載のスクランブル通信システム。

【請求項１９】　前記受信装置は、未受信パケットの偽のパケット識別子を示す否定応答を前記送信装置に送る手段を更に含み、

前記送信装置は、該否定応答に示された偽のパケット識別子に基づいて、該未受信パケットに該当する偽の識別子を有するパケットを再送する手段を更に含む、

ことを特徴とする請求項１１記載のスクランブル通信システム。

【請求項２０】　各パケット中に指定された宛先に対応する次の転送先または最終宛先を示す宛先変換テーブルと、該宛先変換テーブルに基づいて各パケット中に指定された宛先を変更して、該変更された宛先を持つ各パケットを前記ネットワークに転送する転送手段とを含む前記ネットワークに設けられた中継装置、を更に有することを特徴とする請求項１１記載のスクランブル通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、スクランブル通信方法及びシステムに係り、特に、情報の配布に対して課金するような有料情報の提供サービスにおいて、システム（ネットワーク）に非登録端末に対しては情報内容を取得することが困難（読みずらく）にし、登録者にとって配布情報の価値を高めるような情報配布サービスに適用するためのスクランブル通信方法及びシステムに関する。詳しくは、サーバ運用者にスクランブル処理時間の負担をかけることなく、また、端末利用者にもアセンブル（復号）処理の負担をかけることがなく、配布情報のスクランブル配送及び復号を実現するためのスクランブル通信方法及びシステムに関する。

【０００２】

【従来の技術】サーバが端末に対してネットワークを介して情報を配布する時に、登録されていない端末に無断で受信され、利用されることを防ぐためには、送信するデータを分割し、かつ送信する順序を替えて（スクランブルをかけて）、受信後に利用者が事前に配布されている鍵で受信データを復元する方法がある。

【０００３】図１は、従来のスクランブル配送のためのデータ転送方式を説明するための図である。同図に示すシステムは、サーバ１１００、端末１２００及びそれらを接続する通信ネットワーク１３００より構成れる。サーバ１１００は、送信するデータのスクランブル処理を行うアプリケーション１１１０、スクランブル処理されたデータを送信するデータ送信部１１２０、通信制御部１１３０により構成される。端末１２００は、受信したデータに復元処理を行うアプリケーション部１２１０、スクランブル処理されたデータを受信するデータ受信部１２２０、通信制御部１２３０より構成される。

【０００４】同図に示すシステムでは、サーバ１１００のアプリケーション部１１１０において送信前に送信すべき元のデータA全体にスクランブル処理を行い、データA'を生成し、データ送信部１１２０でデータA'を転送データ単位（パケット）に分割し、通信制御部１１３０及び通信ネットワーク１３００を介して端末１２００に送信する。端末１２００は、転送データ単位（パケ

トに格納して該パケットにスクランブルしたパケット順序を示す偽のパケット識別子を付与して該パケットを組み立て、該パケットを該偽のパケット識別子に基づいてスクランブルしたパケット順序でネットワークに送信することにより、該元のデータをスクランブルするステップと、受信側において、前記偽のパケット識別子から真のデータ単位順序を示すデータ単位順序情報を復元し、前記パケットに格納された前記データ単位から該データ単位順序情報に基づいて前記元のデータを再構成することにより、ネットワークから受信した前記パケットを復元するステップと、を有することを特徴とするスクランブル通信方法を提供する。

【００２６】さらに、本発明では、前記スクランブルするステップは、スクランブルされていないパケット順序を示す真のパケット識別子を前記パケットに付与し、所定のスクランブルキーに基づいて該真のパケット識別子を前記偽のパケット識別子に置き換えることにより該パケットを組み立て、前記復元するステップは、前記所定のスクランブルキーに対応する所定のアセンブルキーに基づいて前記偽のパケット識別子を前記真のパケット識別子に変換し、前記元のデータを再構成するにあたって該真のパケット識別子を前記データ単位順序情報として用いることにより該データ単位順序情報を復元する、ことを特徴とする。

【００２７】さらに、本発明では、前記スクランブルするステップは、所定の計算手順に基づいて前記データ単位のメモリアドレスから前記偽のパケット識別子を直接計算して前記パケットを組み立て、前記復元するステップは、前記所定の計算手順に基づいて前記の偽パケット識別子から前記データ単位のメモリアドレスを直接計算し、前記元のデータを再構成するにあたって該メモリアドレスを前記データ単位順序情報として用いることにより該データ単位順序情報を復元する、ことを特徴とする。

【００２８】さらに、本発明では、前記スクランブルするステップは、送信側におけるプロトコル処理により行われることを特徴とする。

【００２９】さらに、本発明では、前記復元するステップは、受信側におけるプロトコル処理により行われることを特徴とする。

【００３０】さらに、本発明では、前記スクランブルするステップは、前記パケットを送信する処理中に利用可能な空き時間を利用して前記元のデータの分割と前記パケットの組み立てを行うことを特徴とする。

【００３１】さらに、本発明では、前記復元するステップは、前記パケットを受信する処理中に利用可能な空き時間を利用して前記データ単位順序情報の復元と前記元のデータの再構成を行うことを特徴とする。

【００３２】さらに、本発明では、前記スクランブルするステップは、所定の数の前記パケットをまとめて送信し、前記元のデータが該所定の数で割切れないときには、該スクランブルするステップは、少なくとも一つのパディングパケットを挿入してまとめて送信する該所定の数のパケットを形成することにより該パケットを組み立てることを特徴とする。

【００３３】さらに、本発明では、受信側から送信側に、未受信のパケットの偽のパケット識別子を示す否定応答を送るステップと、送信側から受信側に、該否定応答に示された偽のパケット識別子に基づいて、該未受信パケットに該当する偽の識別子を有するパケットを再送するステップと、を更に有することを特徴とする。

【００３４】さらに、本発明では、ネットワークに設けられた中継装置において、該中継装置に設けられ、各パケット中に指定された宛先に対応する次の転送先または最終宛先を示す宛先変換テーブルに基づいて、各パケット中に指定された宛先を変更して、送信側から送信された前記パケットを中継するステップ、を更に有することを特徴とする。

【００３５】また、本発明は、ネットワークと、元のデータをパケットサイズの複数のデータ単位に分割し、該データ単位をパケットに格納して該パケットにスクランブルしたパケット順序を示す偽のパケット識別子を付与して該パケットを組み立てることにより該元のデータをスクランブルするスクランブル処理手段と、該パケットを該偽のパケット識別子に基づいてスクランブルしたパケット順序でネットワークに送信する送信手段と、を含む前記ネットワークに接続された送信装置と、前記ネットワークから前記パケットを受信する受信手段と、前記偽のパケット識別子から真のデータ単位順序を示すデータ単位順序情報を復元し、該パケットに格納された前記データ単位から該データ単位順序情報に基づいて前記元のデータを再構成することにより、該パケットを復元する復元処理手段と、を含む前記ネットワークに接続された受信装置と、を有することを特徴とするスクランブル通信システムを提供する。

【００３６】さらに、本発明では、前記スクランブル処理手段は、スクランブルされていないパケット順序を示す真のパケット識別子を前記パケットに付与し、所定のスクランブルキーに基づいて該真のパケット識別子を前記偽のパケット識別子に置き換えることにより該パケットを組み立て、前記復元処理手段は、前記所定のスクランブルキーに対応する所定のアセンブリキーに基づいて前記偽のパケット識別子を前記真のパケット識別子に変換し、前記元のデータを再構成するにあたって該真のパケット識別子を前記データ単位順序情報として用いることにより該データ単位順序情報を復元する、ことを特徴とする。

【００３７】さらに、本発明では、前記スクランブル処理手段は、所定の計算手順に基づいて前記データ単位のメモリアドレスから前記偽のパケット識別子を直接計算

して前記パケットを組み立て、前記復元処理手段は、前記所定の計算手順に基づいて前記偽のパケット識別子から前記データ単位のメモリアドレスを直接計算し、前記元のデータを再構成するにあたって該メモリアドレスを前記データ単位順序情報として用いることにより該データ単位順序情報を復元する、ことを特徴とする。

【００３８】さらに、本発明では、前記スクランブル処理手段は、前記元のデータの分割と前記パケットの組み立てをプロトコル処理を実行することにより行うことを特徴とする。

【００３９】さらに、本発明では、前記復元処理手段は、前記データ単位順序情報の復元と前記元のデータの再構成をプロトコル処理を実行することにより行うことを特徴とする。

【００４０】さらに、本発明では、前記スクランブル処理手段は、前記送信手段による前記パケットを送信する処理中に利用可能な空き時間を利用して前記元のデータの分割と前記パケットの組み立てを行うことを特徴とする。

【００４１】さらに、本発明では、前記復元処理手段は、前記受信手段による前記パケットを受信する処理中に利用可能な空き時間を利用して前記データ単位順序情報の復元と前記元のデータの再構成を行うことを特徴とする。

【００４２】さらに、本発明では、前記送信手段は、所定の数の前記パケットをまとめて送信し、前記元のデータが該所定の数で割切れないときには、前記スクランブル処理手段は、少なくとも一つのパディングパケットを挿入してまとめて送信する該所定の数のパケットを形成することにより該パケットを組み立てることを特徴とする。

【００４３】さらに、本発明では、前記受信装置は、未受信パケットの偽のパケット識別子を示す否定応答を前記送信装置に送る手段を更に含み、前記送信装置は、該否定応答に示された偽のパケット識別子に基づいて、該未受信パケットに該当する偽の識別子を有するパケットを再送する手段を更に含む、ことを特徴とする。

【００４４】さらに、本発明では、各パケット中に指定された宛先に対応する次の転送先または最終宛先を示す宛先変換テーブルと、該宛先変換テーブルに基づいて各パケット中に指定された宛先を変更して、該変更された宛先を持つ各パケットを前記ネットワークに転送する転送手段とを含む前記ネットワークに設けられた中継装置、を更に有することを特徴とする。

【００４５】

【発明の実施の形態】まず、図４から図７を参照して、本発明のスクランブル通信方法およびシステムの主要な特徴について説明する。

【００４６】図４は本発明のスクランブル通信システムの基本構成を示しており、このシステムでは、送信側はデータを提供するアプリケーション１０とスクランブル処理（Ｓ３）と送信処理（Ｐ１（Ｓ１）、Ｐ２（Ｓ２））を行うプロトコル処理部２０を有し、受信側は受信処理（Ｒ１（Ｄ２））と復元処理（Ｄ１）を行うプロトコル処理部４０とデータを取得するアプリケーション５０とを有し、送信側と受信側は通信ネットワーク３０を介して接続される。

【００４７】各部で行われる処理は、図５に示すように、以下の通りである。

【００４８】（ａ）スクランブルしながらパケット送信処理

Ｐ１（Ｓ１）：データ全体をスクランブルに適当な分割サイズに等しいパケットサイズに分割する。図５中で各分割データにつけられた数字は各分割データを識別するための分割データのシーケンス番号である。

【００４９】Ｐ２（Ｓ２）：パケットを組み立てる。

【００５０】Ｓ３：偽のパケット識別番号ｐｆｘを各パケットに付与する。

【００５１】その後パケットは送信側から通信ネットワーク３０に送信され、受信側で受信される。一般に、受信パケットはネットワーク中で順序が入れ替わり、送信した通りの順序で受信側には届かない。

【００５２】（ｂ）復元しながらパケット受信処理

Ｄ１：各パケットの真のパケット識別番号ｐｘを復元しながら、パケットを受信する。

【００５３】Ｒ１（Ｄ２）：パケットから元のデータを再構成する。

【００５４】この本発明のスクランブル通信方法では、スクランブル処理Ｓ１，Ｓ２は送信処理Ｐ１，Ｐ２の一部として行い、復元処理Ｄ２は受信処理Ｒ１の一部として行われる。従って、スクランブル配送を行う場合でも、Ｓ１，Ｓ２およびＤ２の処理はプロトコル処理により行われるので、これらの処理に追加の処理量や処理時間を必要としない。このため、本発明では、スクランブル処理と復元処理をプロトコル処理の一部として実行することによりスクランブル処理と復元処理の大半（Ｓ１，Ｓ２，Ｄ２）にかかる処理量と処理時間を削減することが可能となる。

【００５５】より詳細には、以下に詳述する本発明のスクランブル通信の第１の実施形態では、スクランブル通信は図６に示すように、以下の通り行われる。

【００５６】即ち、スクランブルしながらのパケット送信処理では、Ｐ１（Ｓ１）で、データ全体をスクランブルに適当な分割サイズに等しいパケットサイズに分割する。

【００５７】そして、Ｐ２（Ｓ２）で、各パケットに真のパケット識別番号ｐｘを付与しながらパケットを組み立てる。

【００５８】そして、Ｓ３で、真のパケット識別番号ｐｘを偽のパケット識別番号ｐｆｘで置き換える。

【００５９】一方、復元しながらのパケット受信処理では、Ｄ１で、偽のパケット識別番号ｐｆｘを真のパケット識別番号ｐｘに変換しながらパケットを受信する。

【００６０】そして、Ｒ１（Ｄ２）で、真のパケット識別番号に基づいてパケットから元のデータ全体を再構成する。

【００６１】これに対して、以下に詳述する本発明のスクランブル通信の第２の実施形態では、スクランブル通信は図７に示すように、以下の通り行われる。

【００６２】即ち、スクランブルしながらのパケット送信処理では、Ｐ１（Ｓ１）で、データ全体をスクランブルに適当な分割サイズに等しいパケットサイズに分割する。

【００６３】そして、Ｐ２（Ｓ２）とＳ３で、偽のパケット識別番号ｐｆｘを各パケット中の分割データのメモリアドレスから直接計算して各パケットに付与しながらパケットを組み立てる。

【００６４】一方、復元しながらのパケット受信処理では、Ｄ１で、偽のパケット識別番号ｐｆｘから分割データのメモリアドレスを直接計算しながらパケットを受信する。

【００６５】そして、Ｒ１（Ｄ２）て、分割データのメモリアドレスに基づいてパケットから元のデータ全体を再構成する。

【００６６】次に、図８から図１４を参照して、本発明のスクランブル通信方法およびシステムの第１の実施形態について詳細に説明する。

【００６７】図８は、本発明の第１の実施形態を適用する情報配送システムの構成を示す。同図に示すシステムは、サーバ１００、複数の端末２００－１、２００－２、２００－ｎとこれらを接続するネットワーク３００より構成される。サーバ１００は、ネットワーク３００を介して、複数の端末２００－１、２００－２、２００－ｎに対して、スクランブル処理されたデータを送信し、端末２００において、それぞれ受信したデータを復号する。

【００６８】図９は、第１の実施形態のデータ転送におけるスクランブル配送を説明するための図である。サーバ１００は、アプリケーション部１１０、データ送信部１２０、通信制御部１３０より構成される。

【００６９】アプリケーション部１１０は、端末２００に送信すべきデータ全体をデータ送信部１２０に渡す。

【００７０】データ送信部１２０は、データ全体をパケットに分割し、所定のスクランブルキーに基づいて、シーケンス番号（識別番号）を入れ替えて、通信制御部１３０に転送する。

【００７１】図１０は、図９のサーバ１００におけるデータ送信部１２０の構成を示す。データ送信部１２０は、例えば１ファイル分のデータをアプリケーション部１１０から渡されると、当該ファイルのデータをパケットに分割する処理を行う。データ送信部１２０は、パケット分割部１２１、スクランブルキー格納部１２２、及びスクランブル処理部１２３及び空き時間監視部１２４より構成される。パケット分割部１２１は、アプリケーション部１１０から渡された全データをパケット単位に分割して、スクランブル処理部１２３に転送する。スクランブルキー格納部１２２は、端末２００と共有するスクランブルキーを保持する。スクランブル処理部１２３は、スクランブルキー格納部１２２を参照して、パケット分割部１２１で分割されたパケット単位にスクランブルキーに基づいてパケットシーケンス番号を付与して、図１１に示すようなフォーマットのデータパケットを生成する。

【００７２】図１１に示すデータパケット４００は、宛先４０１、パケットシーケンス番号４０２及びユーザデータ部４０３より構成され、宛先４０１には、受信装置の宛先アドレスを設定し、パケットシーケンス番号４０２には、スクランブル処理部１２３で取得したパケットシーケンス番号を設定し、ユーザデータ部４０３には、分割された１単位分のデータ（メッセージ）を設定する。なお、宛先４０１が付与されない場合には、データは、通信階層上、下階層のパケットに格納される。

【００７３】なお、空き時間監視部１２４については、後述する。

【００７４】サーバ１００の通信制御部１３０は、データ送信部１２０で生成されたデータパケット４００をネットワーク３００を介して端末２００に送信する。

【００７５】端末２００は、アプリケーション部２１０、データ受信部２２０及び通信制御部２３０より構成される。

【００７６】通信制御部２３０は、サーバ１００から転送されたデータパケット４００を受信して、当該パケットをデータ受信部２２０に転送する。

【００７７】データ受信部２２０は、所定のアセンブル（復号）キーによりデータパケット４００のパケットシーケンス番号４０２を復号しながら、データ全体を再構成し、アプリケーション部２１０に転送する。

【００７８】図１２は、図９の端末２００におけるデータ受信部２２０の構成を示す。データ受信部２２０は、復号部２２１、アセンブルキー格納部２２２、データ結合部２２３及び空き時間監視部２２４より構成される。

【００７９】アセンブルキー格納部２２２は、サーバ１００と共有するデータパケット４００のパケットシーケンス番号４０２を復号するためのアセンブルキーを格納している。復号部２２１は、通信制御部２３０より渡されたデータパケット４００に対しアセンブルキー格納部２２２のアセンブルキーを参照して、パケットシーケンス番号４０２を復号する。

【００８０】データ結合部２２３は、復号部２２１で復号された、データパケットを保持しておき、全てのデー

タパケット４００を受け取った時点で、シーケンス番号に基づいてパケットを正規のデータの順に並べ替えて元のデータ（サーバ側のデータ）を再構成する。

【００８１】なお、空き時間監視部２２４については、後述する。

【００８２】この第１の実施形態では、上記の送信前と受信後の処理をサーバ１００の送信処理の空き時間及び端末２００の受信処理の空き時間に行う。空き時間は、サーバ１００及び端末２００の空き時間監視部１２４，２２４がそれぞれの通信制御部１３０、２３０を監視して送信処理またはは受信処理を行っていない時間（空き時間）を検出する。空き時間が検出されると、サーバ１００の空き時間監視部１２４は、パケット分割部１２１を起動し、また、端末２００の空き時間監視部２２４は、復号部２２１を起動する。

【００８３】図１３は、第１の実施形態におけるサーバ側のデータ送信の空き時間を示し、図１４は、第１の実施形態における端末側のデータ受信の空き時間を示す。図１３は、サーバ１００側において、パケットをｎ個連続転送し、一定時間待つという送信速度調整を行っている場合の送信空き時間を例示している。図１４は、端末２００側において、各パケットの受信処理の間の空き時間、及び未受信のパケットがあるため、次のパケットを待っている間にタイムアウトした場合のタイムアウトまでの空き時間を例示している。後者の場合、端末２００では、タイムアウト後にサーバ１００への応答生成処理を行っている。したがって、サーバ１００のデータ送信部１２０は、図１３において、送信空き時間ａ，ｂ，ｃの間で、上記の送信前の処理を行って、端末２００に送信するデータパケット４００を生成する。また、端末２００のデータ受信部２２０は、図１４において、受信空き時間ｘ，ｙ，ｚの間で上記の受信後の処理を行って、サーバ１００から受け取ったデータパケットの復号処理を行う。

【００８４】ここで、以下の説明で用いる用語をいくつか定義しておく。

【００８５】以下の説明において、サーバ１００のアプリケーション部１１０から送信を指示されたデータ全体をメッセージと呼ぶ。また、メッセージを分割して転送するデータの単位をデータパケットと呼ぶ。

【００８６】データパケットは、前述の図１１に示す構成であり、メッセージを分割した情報をユーザデータ部４０３に格納し、メッセージの先頭から対応付けてパケットシーケンス番号４０２を１から順に付与する。データパケットには宛先４０１を付けない場合には、データは、通信階層上、下位層のパケットに格納されて端末に配布される。

【００８７】データパケットの長さは、必要とするスクランブルの粒度（細かさ）に応じて設定する。長さを短くすればするほど、情報がより解読しにくくなる。以下では、６４パケット単位のブロック内のスクランブル転送の例を示すが、このブロックを構成するパケット数を大きくすることにより、情報がより解読しにくくなる。

【００８８】スクランブルキーは、サーバ１００が所有し、復元のためのアセンブルキーは、サーバ１００が各端末毎に、ファイル転送等の通信によって、または、情報配送サービスに登録されている端末にオフラインによって事前に配布しておく。

【００８９】スクランブル転送が行われていることや、使用したパディングの値についてはサーバ１００から端末２００にコネクション確立要求パケット等の手段で、データ転送前に通知されていることとする。

【００９０】次に、上記の定義に基づいてサーバ１００の送信手順について説明する。

【００９１】転送時に速度調節等によりデータパケット転送の空き時間を利用して以下の操作を行うものとする。

【００９２】（１）６４パケット単位のスクランブル
６４パケットの中で、パケットシーケンス番号を入れ替えて、偽のパケットシーケンス番号を付与する。そして、偽のパケットシーケンス番号の順にデータパケットを転送する処理を６４パケット分繰り返す。

【００９３】（２）パディング
サーバ１００のアプリケーション部１１０から与えられたメッセージが６４で割り切れない場合には、パディングパケット（空きパケット）を挿入して、得られる疑似メッセージを６４の倍数とする。

【００９４】一方、端末２００におけるデータパケットの復号処理は、データ受信部２２０がデータパケットを受信する毎に、受信処理の空き時間にアセンブルキーに基づいてパケットシーケンス番号４０２を真の値に置き換える。

【００９５】次に、第１の実施形態に基づいて、スクランブルキー及びアセンブルキーを使用して、スクランブル配送及び復号を行う具体的な例を説明する。

【００９６】（１）サーバ１００から端末２００へのスクランブル配送：この例では、簡単のために８パケットに基づく説明とする。

【００９７】サーバ１００において、メッセージパケットのシーケンス番号列を“１，２，３，４，５，６，７，８”とし、スクランブルキー格納部１２２に格納されているスクランブルキーを、“６，３，７，２，１，８，４，５”とする。このスクランブルキーは、５番目に位置する“１”によってパケットシーケンス番号“５”のパケットを１番目に送信し、４番目に位置する“２”によってパケットシーケンス番号“４”のパケットを２番目に送信し、…ということを表している。

【００９８】これにより、ネットワーク３００上では、偽のパケットシーケンス番号列は、“１，２，３，４，

5，6，7，8”であるが、真のパケットシーケンス番号列は、“5，4，2，7，8，1，3，6”である。

【0099】上記の例は、8パケットを用いた例であるが、64パケットを用いる場合も同様の手順で行う。

【0100】サーバ100は、空き時間において、このスクランブル配送を繰り返す。最初は、パケットシーケンス番号“1～64”番に対して上記の処理を行い、次に、“65～128”番に対して行う。スクランブルキーは同じで、パケット番号のモジュロ64（64で割った余り、0は64として扱う）に対してスクランブルをかける。この処理を64パケット単位に全てのデータに対して行う。

【0101】（2）端末200における復号

受信側の端末200が上記のパケットシーケンス番号列、“1，2，3，4，5，6，7，8”のパケットを受信すると、端末200のアセンブルキー格納部222で保持するアセンブルキーは、“5，4，2，7，8，1，3，6”であり、これは真のパケットシーケンス番号列と同じである。このアセンブルキーは、スクランブルキーより容易に生成可能である。このアセンブルキーは、1番目に位置する“5”によって偽のパケットシーケンス番号“1”を真のパケットシーケンス番号“5”に置き換えて受信し、2番目に位置する“4”によって偽のパケットシーケンス番号“2”を真のパケットシーケンス番号“4”に置き換えて受信し…ということを表している。この復号処理を受信した全てのパケットについて行う。

【0102】（3） 再送のための応答：サーバ100が端末200の未受信パケットに対して再送を行う処理を説明する。

【0103】端末200は、サーバ100に対する応答に未受信パケットの偽のパケットシーケンス番号を入れてサーバ100に送出する（否定応答）。これにより、サーバ100は、再送パケットについても最初のデータ転送と同じスクランブル処理されているものを再送する。

【0104】（4） 受信後の処理

端末200のデータ結合部223は、メッセージ全体を受信後、パディングパケットを取り除き、真のパケットシーケンス番号に従って正規の順に並び替えを行い、元のメッセージを得る。

【0105】尚、上述した第1の実施形態では、サーバ100、端末200の双方に本発明を適用した例を示したが、上記の端末200のパケット受信以降の処理を直ちに行なわずに、単に利用者に配布情報を渡して、その後利用者が別アプリケーション等でアセンブルキーを利用して情報を復元し、最後にメッセージが所定のパケット数で割り切れない場合に用いるパディングパケットを取り除いて、元の情報を得るようにすることも可能である。これは、同一の端末を登録利用者も非登録利用者も使用するような場合に有効である。

【0106】これにより、復号処理に関する負担は利用者にかかるものの、非登録利用者による配布情報の利用を防ぎ、登録利用者に対してのみ有料情報の配布が可能となる。

【0107】次に図15と図16を参照して、本発明のスクランブル通信方法およびシステムの第2の実施形態について詳細に説明する。

【0108】この第2の実施形態においては、情報配送システムの構成は図8に示すものと同じであり、サーバ100と端末200の構成も図9に示すものと同じである。

【0109】図15は、第2の実施形態におけるサーバ100のデータ送信部120の構成を示す。同図に示すデータ送信部120は、パケット組み立て部125とスクランブルキー格納部122より構成される。データ送信部120のパケット組み立て部125は、サーバ100のアプリケーション部110のメモリ上からデータ単位を取り出して、宛先、偽のパケットシーケンス番号を付与してデータパケットを生成する。これにより、予め生成したデータパケットに対してパケットシーケンス番号の変換処理を行う第1の実施形態の場合に比べて、変換処理が不要となる分だけ処理負荷、処理時間が少なくて済む。

【0110】即ち、パケットシーケンス番号を付けてデータパケットを生成するという通信のために必要な手順（処理）に、偽のパケットシーケンス番号を付けるというスクランブルの手順（処理）が一体的に含まれるので、この分の処理が少なくて済むことになる。

【0111】図16は、第2の実施形態における端末200のデータ受信部220の構成を示す。同図に示すデータ受信部220は、パケット分割部225とアセンブルキー格納部222より構成される。データ受信部220において、復号を行う際に、受信したデータ単位の偽パケットシーケンス番号から真のデータ格納位置（メモリアドレス）を算出して、データ受信を行うので、一旦受信データを蓄積してからデータ単位を真のデータ格納位置に並べ替える従来の場合に比べて、データ単位並べ替え処理が不要となる分だけ処理負荷、処理時間が少なくて済む。

【0112】即ち、受信データパケットのパケットシーケンス番号によりデータを格納するという通信のために必要な手順（処理）に真のデータ格納位置を復元するというアセンブルの手順（処理）が一体的に含まれるため、この分の処理が少なくて済むことになる。

【0113】ここで、サーバ100におけるデータ単位のメモリアドレスから偽のパケットシーケンス番号を求める計算と、端末200における偽のパケットシーケンス番号からデータ単位の真のメモリアドレスを求める計算には、以下のような処理負荷の殆どない単純な計算を

用いることができる。ここでも、簡単のために前述同様8パケットに基づく説明とする。

【0114】即ち、サーバ100のスクランブルキー格納部122に格納されているスクランブルキーに対応する、端末200のアセンブルキー格納部222に格納されている真のパケットシーケンス番号列（アセンブルキー）“5，4，2，7，8，1，3，6”に基づいて、サーバ100のデータ送信部120では、偽のパケットシーケンス番号pf1からpf8で送信されるデータ単位のメモリアドレスは、先頭メモリアドレスIとデータ単位サイズdを用いて、次のように順に求められる。

【0115】

偽のパケットシーケンス番号	メモリアドレス
pf1	I＋(5－1)d
pf2	I＋(4－1)d
pf3	I＋(2－1)d
pf4	I＋(7－1)d
pf5	I＋(8－1)d
pf6	I＋(1－1)d
pf7	I＋(3－1)d
pf8	I＋(6－1)d

同様に、偽のパケットシーケンス番号pf9からpf16に対して、対応するメモリアドレスは次のように求められる。

【0116】

偽のパケットシーケンス番号	メモリアドレス
pf9	I＋(8＋4)d
pf10	I＋(8＋3)d
pf11	I＋(8＋1)d
pf12	I＋(8＋6)d
pf13	I＋(8＋7)d
pf14	I＋(8＋0)d
pf15	I＋(8＋2)d
pf16	I＋(8＋5)d

一般には、偽のパケットシーケンス番号pf（8n＋1）からpf（8n＋8）に対応するメモリアドレスは、次のように表される。但し、nは0以上の整数とする。

【0117】

偽のパケットシーケンス番号	メモリアドレス
pf（8n＋1）	I＋(8n＋4)d
pf（8n＋2）	I＋(8n＋3)d
pf（8n＋3）	I＋(8n＋1)d
pf（8n＋4）	I＋(8n＋6)d
pf（8n＋5）	I＋(8n＋7)d
pf（8n＋6）	I＋(8n＋0)d
pf（8n＋7）	I＋(8n＋2)d
pf（8n＋8）	I＋(8n＋5)d

端末200のデータ受信部220では、サーバ100と同じ計算手順を共有することにより、上述した端末200のアセンブルキー格納部222に格納されている真のパケットシーケンス番号列（アセンブルキー）に基づいて、データ単位の真のメモリアドレスを上記の対応に従って偽のパケットシーケンス番号から求めることができる。これにより、データ単位はサーバ100と端末200で同一のメモリアドレスを持つことが可能となる。

【0118】但し、前述した端末200でパケット受信以降の処理を行わずに、単に利用者に配布情報を渡して、その後、利用者側でアセンブルキーを利用して情報を復元し、パディングパケットを除去して元の情報に復元するような場合には、上記のようなデータ格納方法を用いない。

【0119】上記のように、第2の実施形態では、サーバ100のパケット組み立て部125において、端末200と共通に与えられている計算手順を用いることにより、データ単位のメモリアドレスから直接偽のパケットシーケンス番号を取得して、これをデータパケットに付与し、また、端末200のパケット分割部225において、サーバ100と共通に与えられている計算手順を用いることにより、偽のパケットシーケンス番号から直接データ単位の真のデータ格納位置を取得して、当該位置にデータを格納する。

である。ネットワーク７００ａは、企業本店内の中継装置または、端末装置Ａを有し、ネットワーク７００ｆは企業支店内の中継装置または端末装置Ｄを有する。ネットワーク７００ｃは中継装置Ｂと中継装置Ｃを有する。

【０１４０】このような情報ネットワークシステムにおいて、ネットワーク７００ａの企業本店内の端末Ａとネットワーク７００ｆの端末Ｄ間において通信を行う場合に、長距離ネットワーク７００ｃの中継装置と企業の端末Ａ、Ｄとの間に本発明を適用する。このとき、利用者企業と長距離ネットワーク７００ｃとの間に公開接続点や安全が保証されない地域ネットワーク７００ｂを組む場合に、以下のようにして通信を行うことが考えられる。

【０１４１】（１）企業本店の端末Ａと長距離ネットワーク７００ｃの中継装置Ｂとの間で本発明を適用してスクランブル通信を行うことが可能である。

【０１４２】（２）長距離ネットワーク７００ｃは多数の接続点を公開しており、不正アクセスの可能性があるので、長距離ネットワーク７００ｃの中継装置Ｂ－Ｃ間に本発明を適用してスクランブル通信を行うことが可能である。

【０１４３】（３）長距離ネットワーク７００ｃと地域ネットワーク７００ｅの中継装置Ｅ－Ｃ間に本発明を適用してスクランブル通信を行うことが可能である。

【０１４４】このように、あるネットワーク毎に順次本発明によるスクランブル通信を適用していくことにより、秘匿性を保証することが可能となる。

【０１４５】以上の説明では、Ａ、Ｄを企業内の端末として説明したが、Ａ、Ｄを企業内の中継装置とし、Ａ、Ｄを企業内の複数の端末に接続して通信を行う場合にも本発明を同様に適用できる。

【０１４６】なお、本発明は、上記の実施形態に限定されることなく、特許請求の範囲内で種々変更・応用が可能である。

【０１４７】

【発明の効果】以上説明したように、本発明のスクランブル通信方法およびシステムによれば、スクランブル処理と復元処理をプロトコル処理の一部として実行することによりスクランブル処理と復元処理の大半にかかる処理量と処理時間を削減することが可能となるので、送信側や受信側におけるスクランブル処理や復元処理に必要な処理量や処理時間を軽減することが可能となる。

【０１４８】また、本発明のスクランブル通信方法およびシステムによれば、ネットワーク中の適当な箇所に個別にスクランブル通信を適用して中継装置を介在させた通信を行うことにより、複数のネットワークが接続された複合的なネットワークを用いる場合に信頼性の高い情報通信サービスを実現するとが可能となる。

【図面の簡単な説明】

【図１】従来のスクランブル通信システムを示すブロック図。

【図２】従来のスクランブル通信システムの機能構成を示すブロック図。

【図３】従来のスクランブル通信方法の処理の流れを示す図。

【図４】本発明のスクランブル通信システムの機能構成を示すブロック図。

【図５】本発明のスクランブル通信方法の処理の流れを示す図。

【図６】本発明のスクランブル通信方法の第１の実施形態における処理の流れを示す図。

【図７】本発明のスクランブル通信方法の第２の実施形態における処理の流れを示す図。

【図８】本発明の第１、第２の実施形態における情報配送システムを示すブロック図。

【図９】本発明の第１、第２の実施形態におけるスクランブル通信システムを示すブロック図。

【図１０】本発明の第１の実施形態における図９のスクランブル通信システムのデータ送信部を示すブロック図。

【図１１】本発明で用いるデータパケットのフォーマットを示す図。

【図１２】本発明の第１の実施形態における図９のスクランブル通信システムのデータ受信部を示すブロック図。

【図１３】本発明の第１の実施形態において用いる送信側の空き時間を示す図。

【図１４】本発明の第１の実施形態において用いる受信側の空き時間を示す図。

【図１５】本発明の第２の実施形態における図９のスクランブル通信システムのデータ送信部を示すブロック図。

【図１６】本発明の第２の実施形態における図９のスクランブル通信システムのデータ受信部を示すブロック図。

【図１７】本発明の第３の実施形態における情報配送システムを示すブロック図。

【図１８】本発明の第３の実施形態における図１７の情報配送システムの中継装置を示すブロック図。

【図１９】本発明の第３の実施形態における図１８の中継装置の転送処理部を示すブロック図。

【図２０】本発明のスクランブル通信を適用した電子新聞配送システムを示すブロック図。

【図２１】本発明のスクランブル通信を適用した情報ネットワークシステムを示すブロック図。

【符号の説明】

１０　アプリケーション
２０　プロトコル処理部
３０　通信ネットワーク
４０　プロトコル処理部

【０１２０】次に、図１７から図１９を参照して、本発明のスクランブル通信方法およびシステムの第３の実施形態について詳細に説明する。

【０１２１】上記の第１及び第２の実施形態では、サーバ／端末のエンドエンド間のスクランブル通信の例を示したが、本発明のスクランブル通信は「サーバ／端末」のみならず、「サーバ／中継装置」、「中継装置／中継装置」、「中継装置／端末」等、各装置間の通信に個別に必要に応じて適用できる。

【０１２２】図１７は、本発明の第３の実施形態を適用する中継装置を含む情報配送システムの構成を示す。

【０１２３】同図は、上記の図８のサーバと端末のエンド／エンド間でスクランブル通信を行う構成に加えて、サーバ１００がネットワーク３００内の中継装置３００－１に回線で接続され、中継装置３００－７から３００－ｎ間が回線で接続され、中継装置３００－２と端末２００－１、端末２００－２が接続されている。図１７に示すシステムでは、サーバ／中継装置、中継装置間、中継装置／端末間の各箇所において必要に応じて個別にスクランブル通信を行う。

【０１２４】このようにネットワーク３００内の中継装置を介してスクランブル通信を行うことにより、複合化されたネットワークにおける通信においても秘匿性を保持した通信が可能となる。

【０１２５】なお、図１７において、ネットワーク及びサーバ／中継装置間の回線及び中継装置間の回線及び中継装置／端末間の回線には地上のＩＳＤＮ、専用線等の有線、衛星、セルラ等の無線の各種伝送形態を利用可能である。また、中継装置は、パケット交換機、ＡＴＭ交換機、ルータ等が利用できる。

【０１２６】図１８は、第３の実施形態の中継装置３００－ｎの構成を示す。同図に示す中継装置３００－ｎは、転送処理部３１０、中継受信部３２０及び中継送信部３３０より構成され、中継送信部３２０は、データ送信部３２１と通信制御部３２２より構成され、中継送信部３３０は、データ送信部３３１と通信制御部３３２より構成され、データ受信部３２１及び通信制御部３２２は、図９に示す端末２００のデータ受信部２２０及び通信制御部２３０と同様の機能を有する。転送処理部３１０は、中継するデータパケットの宛先変換処理を行う。

【０１２７】図１９は、図１８の中継装置３００－ｎにおける転送処理部３１０の構成を示す。同図に示す転送処理部３１０は、宛先変換テーブルを格納する宛先変換テーブル格納部３１１、受信したデータパケットを蓄積する転送データバッファ３１２及び、宛先変更処理を実行する転送データ制御部３１３を有する。このような中継装置は、蓄積交換型の中継装置で通常用いられるものである。

【０１２８】このような構成を有する第３の実施形態の中継装置３００－ｎによるデータパケット中継の手順は、次の通りである。

【０１２９】転送処理部３１０において、データ受信部３２１からデータパケットを受け取ると、宛先変換テーブル格納部３１１の宛先変換テーブルを参照して、データパケットの宛先を転送先の中継装置あるいは、最終の配送先の端末２００の宛先に変換する。データ単位が適当数溜ったところで、データ送信部３３１に送信要求する。データ転送部３３１では、相手中継装置あるいは端末２００との間でパケットの転送を行う。

【０１３０】以上の手順における転送処理部３１０の動作は、次の通りである。転送データ制御部３１３は、受信データを転送データバッファ３１２に蓄積し、宛先変換テーブル格納部３１１の宛先変換テーブルを参照してデータパケットの宛先を変更してデータパケットを転送する。

【０１３１】次に、図２０を参照して、情報配送サービス加入者と情報サービスセンタとの間に本発明のスクランブル通信を適用した電子新聞配送システムの例を説明する。

【０１３２】図２０は、本発明を適用した電子新聞配送システムの一例を示す。

【０１３３】同図に示すシステムは、サーバ１００を有する配送センタ５００、通信ネットワーク３００、複数の端末２００、端末２００を有する販売所６００より構成される。

【０１３４】端末２００を持たない購読者には、販売所６００で複製された電子新聞が販売所６００より配布される。

【０１３５】サーバ１００から端末２００にマルチキャスト通信により、毎朝、一斉に電子新聞を配布する。その際、本発明のスクランブル通信方法に従って情報のスクランブルを行う。購読を登録している利用者の端末２００には予め安全な方法で復元鍵（アセンブルキーを表す数字列）を配布しておく。非登録利用者は、通信を傍受することはできても復元鍵がないので、容易に解読することはできない。

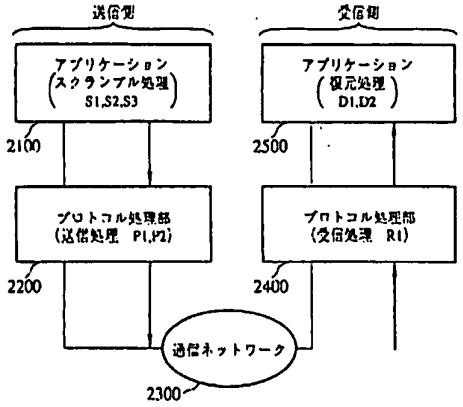
【０１３６】例えば、同図において、端末Ａの利用者は復元鍵２４０を有しているため、当該通信による購読が可能であるが、端末Ｂの非登録利用者は復元鍵を有していないため、購読が不可能である。

【０１３７】なお、復元鍵を定期的に変更し、購読料が未払いの利用者には最新の復元鍵を配布しないようにすることにより、そのような利用者は電子新聞を受信できても解読が困難となるようにすることが可能である。

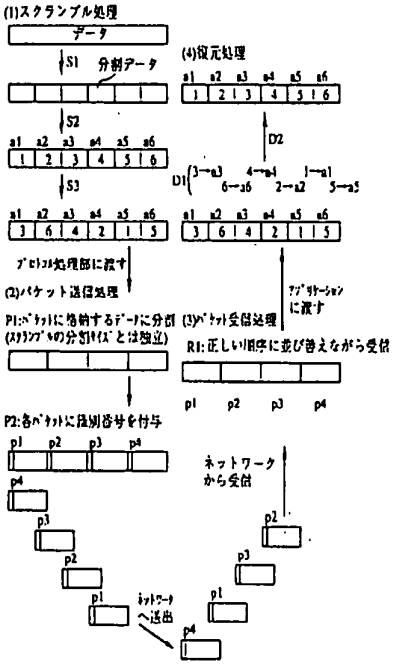
【０１３８】次に、図２１を参照して、本発明のスクランブル通信の情報ネットワークへの部分的な適用を説明する。

【０１３９】図２１は、本発明を部分的に適用した情報ネットワークシステムの一例を示す。同図において、楕円で示される７００ａから７００ｆは情報ネットワーク

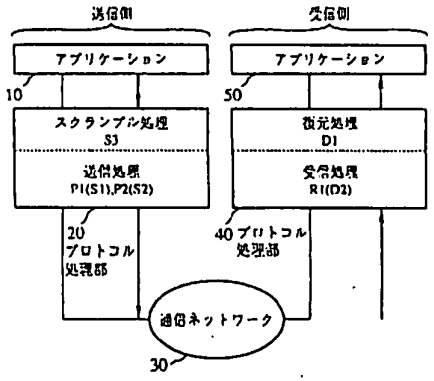
【図2】(従来)



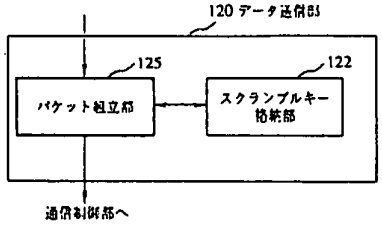
【図3】(従来)



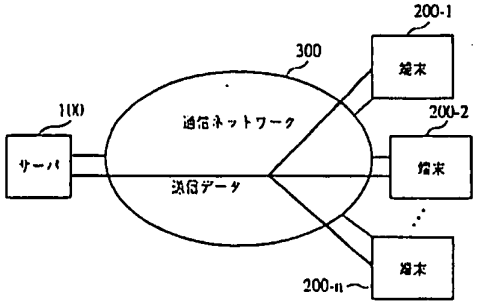
【図4】



【図15】

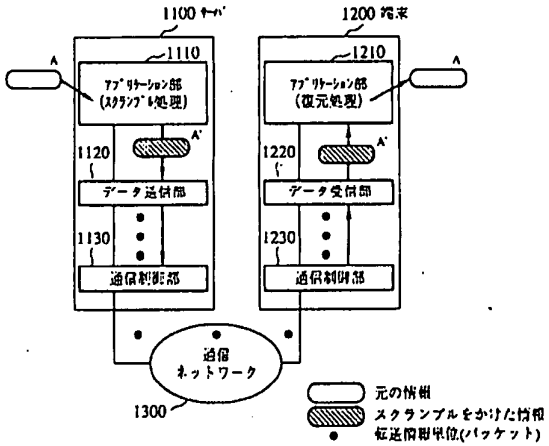


【図8】

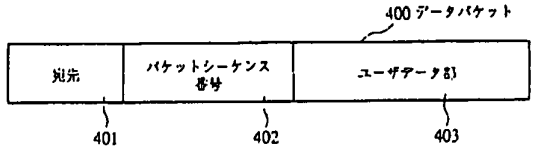


50 アプリケーション
100 サーバ
110 アプリケーション部
120 データ送信部
121 パケット分割部
122 スクランブルキー格納部
123 スクランブル処理部
124 空き時間監視部
125 パケット組み立て部
130 通信制御部
200 端末
210 アプリケーション部
220 データ受信部
221 復号部
222 アセンブルキー格納部
223 データ結合部
224 空き時間監視部
225 パケット分解部
230 通信制御部
240 復元鍵
300 通信ネットワーク
300－1～300－n 中継装置
310 転送処理部
311 宛先変換テーブル格納部
312 転送データバッファ
313 転送データ制御部
320 中継受信部
321 データ受信部
322 通信制御部
330 中継送信部
331 データ送信部
332 通信制御部
400 データパケット
401 宛先
402 パケットシーケンス番号
403 ユーザデータ部
500 配送センタ
600 販売所
700a～700f ネットワーク

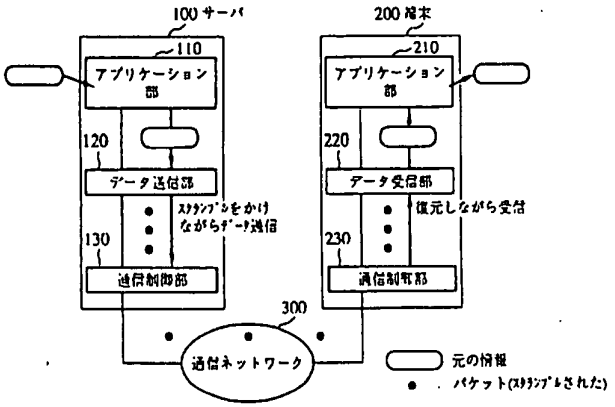
【図1】(従来)



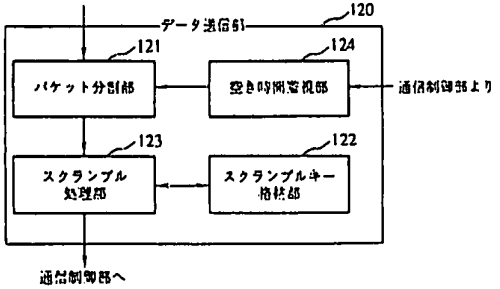
【図11】



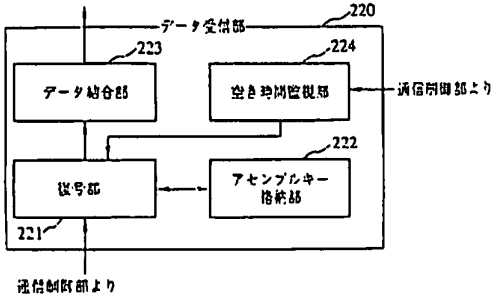
【図9】



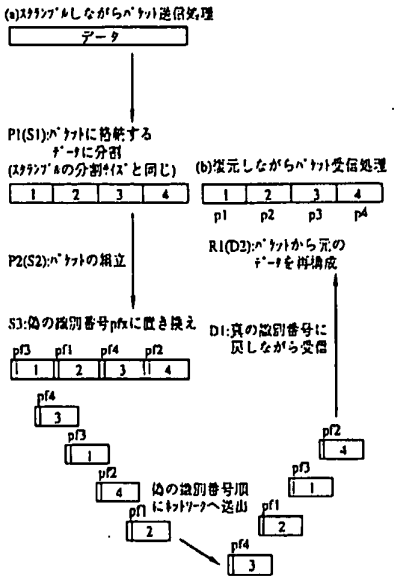
【図10】



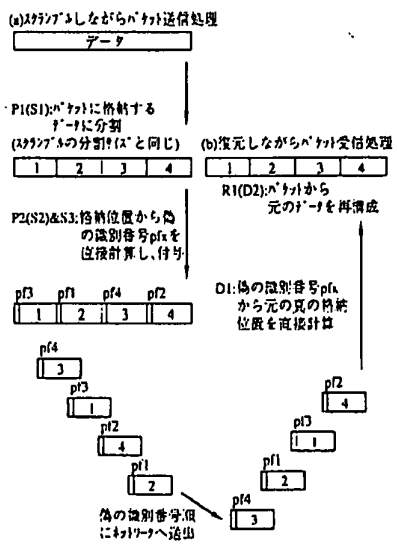
【図12】



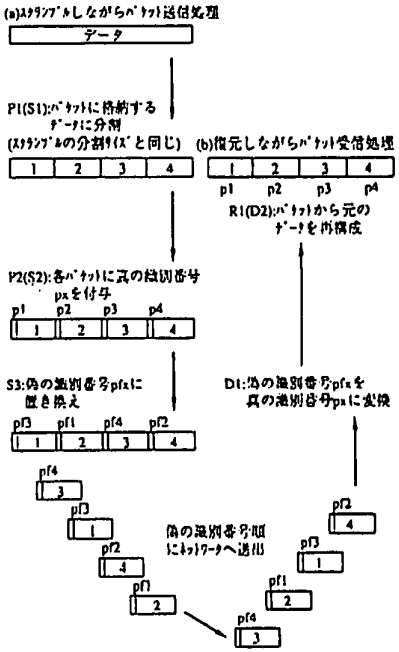
【図5】



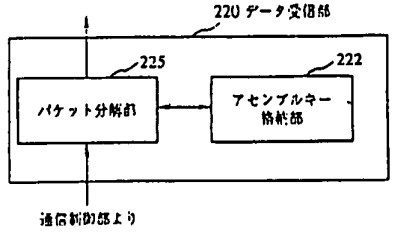
【図7】



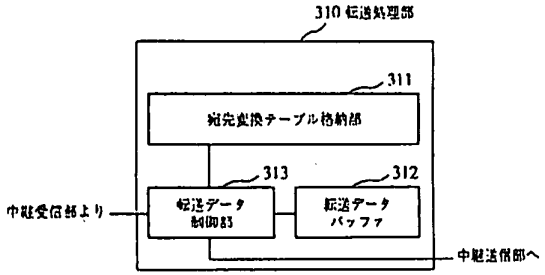
【図6】



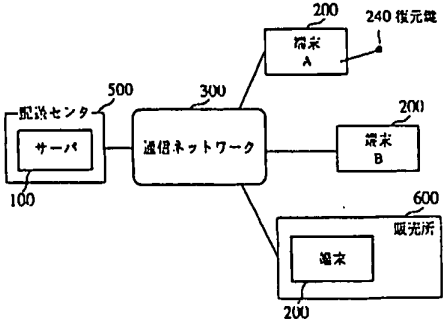
【図16】



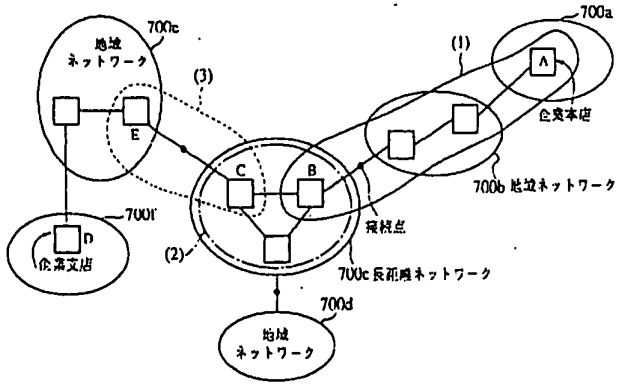
【図１９】



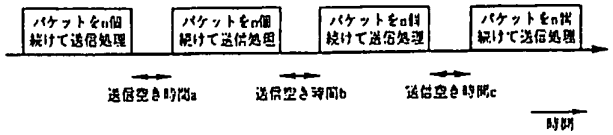
【図２０】



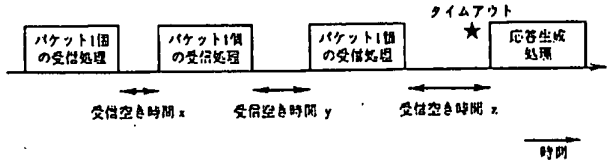
【図２１】



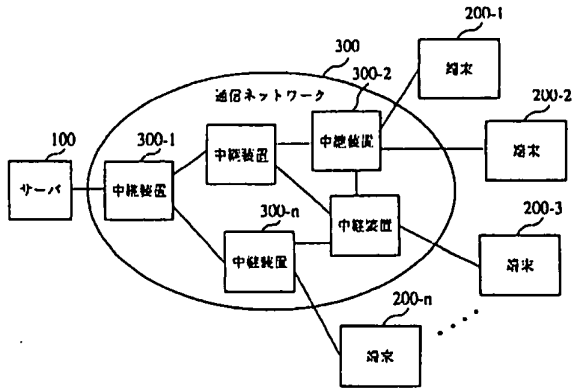
【図１３】



【図１４】



【図１７】



【図１８】